

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problems Mailbox.**



PATENT ABSTRACTS OF JAPAN

(11) Publication number: **06104900 A**(43) Date of publication of application: **15 . 04 . 94**

(51) Int. Cl. **H04L 12/28**
H04L 12/40

(21) Application number: **04252581**(22) Date of filing: **22 . 09 . 92**(71) Applicant: **MATSUSHITA ELECTRIC IND CO LTD**

(72) Inventor: **KITO TSUTOMU**
YAMAGUCHI HIROSHI
NINOBE NAOHISA
TAKEUCHI HIRONORI
MORI TAKASHI
MUSA MUTSUMI

(54) **LAN-TO-LAN CONNECTION METHOD**

(57) Abstract:

PURPOSE: To provide LAN-to-LAN connection method capable of good filtering of high-class data realizing a security function which permits the access only to a specific terminal and inhibits the access to other terminals even when managing a LAN system.

CONSTITUTION: The method is provided with filtering table registering a destination address 11 of the terminal equipment to which data are reached and a transmission source address 12 of the terminal which sends the data. The connection is permitted to only inter-terminal equipment which is registered in the filtering table data connection request from an arbitrary terminal equipment, performing data transmission.

11	宛先アドレス	送信元アドレス	12

COPYRIGHT: (C)1994,JPO&Japio

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開平6-104900

(43)公開日 平成 6 年(1994) 4 月15日

(51)Int.Cl. ⁵	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 L 12/28 12/40		8732-5K 7341-5K	H 0 4 L 11/ 00	3 1 0 C 3 2 0

審査請求 未請求 請求項の数 2 (全 4 頁)

(21)出願番号	特願平4-252581	(71)出願人	000005821 松下電器産業株式会社 大阪府門真市大字門真1006番地
(22)出願日	平成 4 年(1992) 9 月22日	(72)発明者	鬼頭 勉 神奈川県横浜市港北区綱島東四丁目 3 番 1 号 松下通信工業株式会社内
		(72)発明者	山口 広 神奈川県横浜市港北区綱島東四丁目 3 番 1 号 松下通信工業株式会社内
		(72)発明者	ニ之部 直久 神奈川県横浜市港北区綱島東四丁目 3 番 1 号 松下通信工業株式会社内
		(74)代理人	弁理士 小鍛冶 明 (外 2 名)

最終頁に続く

(54)【発明の名称】 LAN間接続方法

(57)【要約】

【目的】 LANシステムを管理する場合でも、特定の端末装置にのみアクセスし、他の端末装置にはアクセスを禁止できるセキュリティ機能を実現する、高度なデータのフィルタができる優れたLAN間接続方法を提供することを目的とする。

【構成】 データを到達すべき端末装置の宛先アドレス 1 1 とデータを送出する端末装置の送信元アドレス 1 2 とを登録するフィルタリングテーブルを設け、任意の端末装置からの接続要求に対して前記フィルタリングテーブルに登録された端末装置間のみ接続を許可し、データの伝送を行う。

1 1	宛先アドレス	送信元アドレス	1 2

フィルタリングテーブル

【特許請求の範囲】

【請求項1】 それぞれ端末装置を接続する複数のLAN間で、データ伝送の経路を決定する宛先IPアドレス及び送信元IPアドレスを登録したルーティングテーブルを参照して接続し、任意のLANに接続された端末装置と他のLANに接続された端末装置との間でデータ伝送を行うときのLAN間接続方法であって、データを到達すべき端末装置の宛先アドレスとデータを送出する端末装置の送信元アドレスとを登録するフィルタリングテーブルを設け、任意の端末装置からの接続要求に対して前記フィルタリングテーブルに登録された端末装置間のみ接続を許可し、データの伝送を行うことを特徴とするLAN間接続方法。

【請求項2】 それぞれ端末装置を接続する複数のLAN間で、データ伝送の経路を決定する宛先IPアドレス及び送信元IPアドレスを登録したルーティングテーブルを参照して接続し、任意のLANに接続された端末装置と他のLANに接続された端末装置との間でデータ伝送を行うときのLAN間接続方法であって、データの伝送を禁止する端末装置のIPアドレスを登録するフィルタリングテーブルを設け、任意の端末装置からの接続要求に対して前記フィルタリングテーブルを参照し、前記フィルタリングテーブルに登録された端末装置への接続を禁止することを特徴とするLAN間接続方法。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明はコンピュータネットワークに利用するLAN間接続方法に関する。

【0002】

【従来の技術】 図2は複数のLAN間を接続してデータ伝送を行うシステムの構成を示すものである。図2において、31はデータ伝送に光ファイバーを使用したFDDI-LANのバックボーンLAN（以下、単にバックボーンという）であり、32、33は複数の異なるLANをバックボーン31に接続するLAN間接続装置である。このLAN間接続装置32、33は、物理層とデータリンク層が異なる複数のLANを、共通のネットワーク層（第3層）で相互接続する。34はFDDI-LANに接続されている共通データベースである。35、36はLANを構成するイーサネットである。イーサネット35及び36には、端末装置37A、37B及び38A、38B、並びに、図には示していない他の端末装置が接続されている。

【0003】 図2のようなシステムにおいて、異なるLANに接続された端末装置間でデータの伝送を行う場合、自由にデータ伝送を行うわけではなく、IP（インターネットプロトコル）に基づいて、データの透過又は遮断を制御するフィルタリングを行うLAN間接続方法が用いられていた。

【0004】 従来のLAN間接続方法においてフィルタ

リングを行う場合に、IPが本来保持しているルーティングテーブルをルーティングプロトコルを通して、もしくは、ルーティングプロトコルのコンフィグレーションを変更して、間接的にルーティングテーブルを書き換えるか、あるいは、ルーティングプロトコルを使用せずに直接、ルーティングテーブルを書き換えるというものであった。図3はルーティングテーブルを示すもので、1は宛先IPアドレスであり、2は送信元IPアドレスである。このIPアドレスは、A、B、Cの3つのクラスを示すビットの他、上位のネットワークアドレス、及び、下位のホストアドレスで構成されている。

【0005】 次に上記従来例の動作について説明する。いま、端末装置37Aから端末装置38BにIPデータを伝送する場合を想定する。まず、端末装置37AからIPデータがLAN間接続装置32に到達すると、LAN間接続装置32は、IPデータを送信する宛先を、図3の宛先IPアドレスを参照して検索する。そしてホストアドレスが同じイーサネット35にあれば、そのIPデータを廃棄する。この場合、ホストアドレスの示す端末装置38Bはイーサネット35にないので、端末装置38Bが接続されたLAN（イーサネットに限らない）をネットワークアドレスにより検索する。次に、をが存在するかどうかを、図3の宛先IPアドレスの欄について検索する。この場合、データを伝送すべき端末装置28Bが接続されたネットワークはイーサネット36であるので、イーサネット36に接続されているLAN間接続装置33を宛先IPアドレスとして、IPデータを伝送する。これを受信したLAN間接続装置33は、宛先IPアドレスのホストアドレスが示す端末装置38BにIPデータを伝送する。

【0006】 LAN間接続装置32又は33において、ルーティングテーブルを参照した結果、一致するIPアドレスがエントリされていない場合には、そのデータは廃棄される。このように、上記従来のLAN間接続方法においてもIPデータのフィルタリングが実現されていた。

【0007】

【発明が解決しようとする課題】 しかしながら、上記従来のLAN間接続方法においては、IPの本来もつルーティングテーブルに依存したフィルタ機能を用いているので、パスワード等のステーションレベルすなわちレイヤ2レベルでのセキュリティは可能であったが、レイヤ3レベルでのセキュリティとしては不十分であった。従って、1つのビル内に複数のテナントがそれぞれLANを構築している場合には、そのビル全体のLANシステムの管理者は、管理する全てのLANに接続された端末装置のアドレスを有するルーティングテーブルをもって、管理する全ての端末装置に自由にアクセスすることができた。そのため、データの盗難やハッカーの侵入を防止することができず、完全なセキュリティ

を実現するには不十分であるという問題があった。

【0008】本発明はこのような従来の問題を解決するものであり、LANシステムを管理する場合でも、特定の端末装置にのみアクセスし、他の端末装置にはアクセスを禁止できるセキュリティ機能を実現する、高度なデータのフィルタができる優れたLAN間接続方法を提供することを目的とするものである。

【0009】

【課題を解決するための手段】本発明は上記目的を達成するために、データを到達すべき端末装置の宛先アドレスとデータを送出する端末装置の送信元アドレスとを登録するフィルタリングテーブルを設け、任意の端末装置からの接続要求に対して前記フィルタリングテーブルに登録された端末装置間のみ接続を許可し、データの伝送を行う。

【0010】また、データの伝送を禁止する端末装置のIPアドレスを登録するフィルタリングテーブルを設け、任意の端末装置からの接続要求に対して前記フィルタリングテーブルを参照し、前記フィルタリングテーブルに登録された端末装置への接続を禁止する。

【0011】

【作用】本発明は上記のような構成により、LAN間接続装置を通過するデータがIPアドレスの組み合わせから、宛先もしくは送信元のネットワークアドレスでフィルタが掛けられるために高度なセキュリティ機能を実現するネットワーク設計が可能になる。

【0012】

【実施例】以下、本発明の実施例を図2に示す構成を援用して説明する。

【0013】本実施例において、共通データベース34は、各イーサネット35及び36からアクセス可能にするが、他のイーサネットにアクセス可能な端末装置をイーサネットごとに制限するような構成とする。例えば、イーサネット35では、端末装置37Aに限り他のイーサネットにアクセス可能とする。また、イーサネット36では、端末装置38Aに限り他のイーサネットにアクセス可能とする。この場合には、LAN間接続装置32に設けたフィルタリングテーブルにおいて、宛先アドレスを38Aとし、送信元アドレスを37Aとする。同様に、LAN間接続装置33に設けたフィルタリングテ

【図1】

宛先アドレス	送信元アドレス

フィルタリングテーブル

*ブルにおいて、宛先アドレスを37Aとし、送信元アドレスを38Aとする。

【0014】このようなエントリを行うことにより、例えば、端末装置38Bから端末装置37Aにアクセスしても接続を行わない。また、送信元アドレスが端末装置38A以外の端末装置場合にも、そのデータをフィルタリングすなわち遮断することができる。従って、このフィルタリングテーブルによってアクセス可能な端末装置を、例えば、トラヒックや課金情報等の管理データのみを格納する部門サーバとして、他の端末装置へはアクセスを禁止することができる。

【0015】このように上記実施例によれば、従来のルーティングテーブルによっては行えないレイヤ3レベルでのフィルタリングが可能であり、データの盗難やハッカーの侵入を防止することができ、状況に応じたセキュリティの要請に応えたネットワークの通信経路設計が可能になるという効果を得ることができる。

【0016】なお、上記実施例においては、接続する端末装置のアドレスをエントリするようにしたが、接続を禁止する端末装置すなわちフィルタリングする端末装置のアドレスをエントリすることにより、エントリした端末装置以外のものに対して、データを伝送する構成としても良い。

【0017】

【発明の効果】本発明は上記実施例より明らかなように、データを伝送する宛先アドレスと送信元アドレスをエントリするフィルタリングテーブルを設けることにより、レイヤ3レベルのセキュリティが可能となり、データの盗難やハッカーの侵入を防止でき、ウィルスの感染をも防御できる優れたLAN間接続方法を実現する効果が得られる。

【図面の簡単な説明】

【図1】本発明のLAN間接続方法に用いるフィルタリングテーブルの図

【図2】複数のLAN間を接続するシステムの構成図

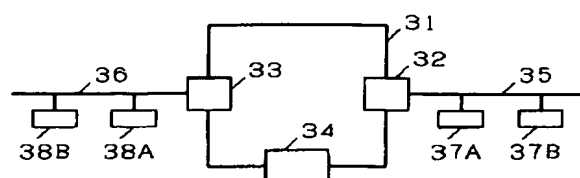
【図3】従来のLAN間接続方法に用いるルーティングテーブルの図

【符号の説明】

11 宛先アドレス

12 送信元アドレス

【図2】



【図3】

1	宛先IPアドレス	送信元アドレス	2

ルーティングテーブル

フロントページの続き

(72)発明者 竹内 宏則
神奈川県横浜市港北区綱島東四丁目3番1
号 松下通信工業株式会社内

(72)発明者 森 孝志
神奈川県横浜市港北区綱島東四丁目3番1
号 松下通信工業株式会社内

(72)発明者 武佐 睦
神奈川県横浜市港北区綱島東四丁目3番1
号 松下通信工業株式会社内